

SIEMENS

PATENT
Attorney Docket No. 2002P15289WOUS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Inventor:	M. Franke et al.)	Group Art Unit: 2139
)	
Serial No.:	10/528,312)	Examiner: Hailu, Teshome
)	
Filed:	03/17/005)	Confirmation No.: 2692
Title:	METHOD FOR GENERATING AND/OR VALIDATING ELECTRONIC SIGNATURES		

Mail Stop Appeal Brief - Patent
Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450
COMMISSIONER FOR PATENTS

APPELLANTS' BRIEF UNDER 37 CFR 41.37

Sir:

This brief is in furtherance of the Notice of Appeal filed in this application on 29 May 2008.

1. REAL PARTY IN INTEREST - 37 CFR 41.37(c)(1)(i)

The real party in interest in this Appeal is the assignee of the present application, Siemens Aktiengesellschaft.

2. RELATED APPEALS AND INTERFERENCES - 37 CFR 41.37(c)(1)(ii)

There is no other appeal, interference or judicial proceeding that is related to or that will directly affect, or that will be directly affected by, or that will have a bearing on the Board's decision in this Appeal.

3. STATUS OF CLAIMS - 37 CFR 41.37(c)(1)(iii)

Claims canceled: 1 - 5, 7, 9, 11, 13, 15, 17, 19 and 21.

Claims withdrawn but not canceled: None.

Claims pending: 6, 8, 10, 12, 14, 16, 18, 20, 22 and 23.

Claims allowed: none.

Claims rejected: 6, 8, 10, 12, 14, 16, 18, 20, 22 and 23.

The claims on appeal are 6, 8, 10, 12, 14, 16, 18, 20, 22 and 23. A copy of the claims on appeal is attached hereto in the Claims Appendix. Appellants respectfully appeal the final rejection of claims 6, 8, 10, 12, 14, 16, 18, 20, 22 and 23.

4. STATUS OF AMENDMENTS - 37 CFR 41.37(c)(1)(iv)

In response to the Final Office Action mailed 29 February 2008, the Appellants submitted a response without amendment under Rule 116 on 28 April 2008. The Examiner entered the Response per the Advisory Action mailed 28 May 2008. The Advisory Action indicates that the grounds of rejection presented in the Final Office Action remain unchanged.

5. SUMMARY OF THE CLAIMED SUBJECT MATTER- 37 CFR 41.37(c)(1)(v)

With reference by page and line number to the detailed description, the following summary references one or more exemplary embodiments described in the Specification and which are covered by specific claims, but it is to be understood that the claims are not so limited in scope.

5A. BRIEF BACKGROUND PROVIDING CONTEXT FOR THE SUMMARY OF CLAIMED SUBJECT MATTER

The invention relates to electronic signatures of the type used to assure authenticity, legal validity and integrity. Such signatures generally require two keys which are mathematically dependent on one another. A private key is used for generating the electronic signature. A public key is used for verifying the signature provided, i.e., by identifying a link between the name of the person to whom the signature relates and the corresponding public key. This link, referred to as a certificate, is issued by a third party, referred to as a certification authority.

Certificates only have a limited period of validity. Certification authorities have separate key pairs for signing certificates, creating black lists and time stamps. Signature methods have included a first algorithm for generating the signature and an associated second algorithm for verifying signatures.

Prior known signature methods have required significant effort to effect permanent protection of the private signature key (by the person to whom the signature is assigned) against unauthorized use. The claimed invention relates to generation of electronic signatures without requiring permanent protection of the private signature key by the person to whom the signature is assigned.

According to an embodiment of the invention, certification of the public validation key need not take place until after calculation of the electronic signature. An intentional action by an author of an electronic document (e.g., expressed by use of the electronic signature) may only take place after signature generation in the context of a certificate request process. Because the intentional action is represented by a certificate request (instead of an initiation of a calculation of an electronic signature) it is not necessary to keep a private signature key which corresponds

to the public signature key after calculation of the electronic signature. Consequently, the private signature can be destroyed following a calculation of the electronic signature. Therefore a need no longer exists for protecting the private signature key against unauthorized access.

Also according to embodiments covered by the claims, when validating an electronic signature only those signatures which were generated at a time prior to the certification of the public validation key are recognized as valid. This has the result of eliminating the revocation problems which relate to public validation keys and are known in the context of previous signature methods. Moreover, this ensures that it is no longer possible to misuse the private signature key after the time of the certification of the public validation key. Therefore no mechanisms for permanently preventing unauthorized accesses to the private signature key are required.

When certifying the public validation key in accordance with the claimed invention, it is possible to include a reference to the relevant signed electronic document in addition to a user identifier and the public validation key. When validating the signature on the recipient side, the reference to the electronic document is also evaluated. Furthermore, it is possible for the certification of the public validation key to include not just one reference to a single electronic document, but a plurality of references to electronic documents which are signed within a specific reference period. A reference to an electronic document may be implemented, for example, by means of a calculated hash value for the relevant electronic document. When validating signatures on the recipient side, corresponding hash values are compared.

5B. CONCISE EXPLANATION OF SUBJECT MATTER DEFINED IN EACH INDEPENDENT CLAIM

5B(i). Summary of Subject Matter Defined In Independent Claim 6.

In accord with Figure 2, **independent claim 6**, directed to a method for generating or validating electronic signatures, includes the steps of

(i) generating an asymmetrical key pair (Step 200) which includes a private signature key 210 and a public validation key (see page 6, line 28 - page 7, line 1; and page 7, lines 7-10);

(ii) calculating an electronic signature for an electronic document by means of the private signature key and by applying a predeterminable signature function (see again page 6, lines 30 - page 7, line 1); and

(iii) performing a certification of the public validation key (see page 7, lines 7 - 30) wherein, when validating, only those signatures generated at a time prior to the certification of the public validation key are recognized as valid. See page 7, line 32 - page 8, line 9.

5B(ii). Summary of Subject Matter Defined In Independent Claim 18

Also in accord with Figure 2, **independent claim 18** is directed to a method for generating or validating electronic signatures. The method includes

(i) generating an asymmetrical key pair (Step 200) which includes a private signature key 210 and a public validation key (see page 6, line 28 - page 7, line 1; and page 7, lines 7-10);

(ii) calculating at least one electronic signature for at least one electronic document by means of the private signature key and by applying a predeterminable signature function (see again page 6, lines 30 - page 7, line 1); and

(iii) following calculation of the electronic signature, of which there is at least one, carrying out a certification of the public validation key wherein only those signatures generated at a time prior to the certification of the public validation key are recognized as valid. See page 7, line 1 - page 8, line 9.

6. GROUNDS OF REJECTION TO BE REVIEWED UPON APPEAL - 37 CFR 41.37(c)(1)(vi)

1. Whether claims 6, 12, 18 and 23 are unpatentable under 35 U.S.C. Section 103 over U.S. Patent No. 6,948,061 (Dierks) in view of U.S. Pub. No. 2002/0108042 (Oka).

2. Whether claims 8, 10, 14, 16, 20 and 22 are unpatentable under 35 U.S.C. Section 103 over Dierks in view of Oka and in further view of U.S. Pub. No. 2002/0108041 (Watanabe).

7. ARGUMENT 37 CFR 41.37(c)(1)(vii)

7A. APPELLANTS TRAVERSE ALL ART REJECTIONS.

With Regard to the Art Rejections, Patentability of Each Claim is to be Separately Considered

Appellant urges that patentability of each claim should be separately considered. All of the claims are separately argued. General argument, based on deficiencies in the rejection of independent claims 6 and 18 under Section 103 demonstrates patentability of all dependent claims. However, none of the rejected claims stand or fall together because each dependent claim further defines a unique combination that patentably distinguishes over the art of record. For this reason, the Board is requested to consider each argument presented with regard to each dependent claim. Argument demonstrating patentability of each dependent claim is presented under subheadings identifying each claim by number.

7A(1) REJECTION OF THE INDEPENDENT CLAIMS 6 AND 18, AND CLAIMS 12 AND 23 WHICH DEPEND THEREFROM UNDER SECTION 103 IS IN ERROR.

The Appellants traverse all of the claim rejections under 35 USC 103 because the combination of Dierks in view of Oka used to reject independent claims 6 and 18 fails to disclose each feature recited in the claims.

7A(1)i REJECTION OF INDEPENDENT CLAIM 6 UNDER SECTION 103 BASED ON DIERKS IN VIEW OF OKA IS IN ERROR.

Application of the combination of Dierks in view of Oka under Section 103 results in deficiencies that render the rejection of claim 6 incorrect. The method of claim 6 requires **performing a certification of the public validation key wherein, when validating,**

“only those signatures generated at a time prior to the certification of the public validation key are recognized as valid.”

Prior to receiving the Final Office Action, Appellants amended claims 6 and 18 to incorporate this language and more fully distinguish over the Dierks reference. At that stage of the prosecution, the Dierks reference had been applied to the same subject matter because the Abstract of Dierks was incorrectly construed as disclosing that only those signatures generated at a time prior to the certification of the public validation key are recognized as valid. In fact, this is not what the reference discloses. In response to Appellants' argument the Final Office Action presented new grounds of rejection, relying upon the Oka reference for what the Dierks reference lacks. But the Oka reference does not compensate for this deficiency.

At page 3, the Final Office Action concludes, incorrectly, that the Oka reference provides what is missing from the Dierks reference. Citing Par. [0152] of Oka it was stated that Oka teaches: “that only the signatures generated prior to the certification of the public key are recognized as valid.”

The rejection goes on to state (see again page 3 of the Final Office Action) that

“the certificate authority (CA) selects signature modules ... and causes the selected modules to generate signatures based on the respective cryptosystems ... before issuing a public key certificate containing the generated signatures.”

However, neither the above statement quoted from the Office Action nor any text in the cited paragraph [0152] disclose the above-recited claimed subject matter (which is also absent from the Dierks reference). At best, this passage only discloses that modules generate signatures before issuing a certificate. This is not the same as requiring that *only those signatures generated at a time prior to the certification of the public validation key are recognized as valid.*

To further illustrate that the prior art combination does not result in the claimed feature, reference is again made to the Dierks reference at col. 3, lines 51-56 which supports applicants' interpretation that the disclosure of Dierks is limited to the prior art and expressly inconsistent with the teachings of the Appellants. The passage states that the validation engine has the ability to allow the completion of a requested private key operation by determining

“whether a certificate is treated as valid at that moment or instant in time ...”

Thus the reference does not obtain a certificate for each request, but only determines whether the certificate is still considered valid. In contrast to such, the invention as defined in independent claim 6 never permits a certificate to be treated as valid unless

“the signatures generated at a time prior to the certification of the public validation key are recognized as valid.”

Consequently, the claimed invention is different, e.g., because the Dierks reference expressly teaches at col. 3, line 67 – col. 4, line 4, that

“the message may only be encrypted if the certificate is valid at the time of encryption ...”

It would be necessary to reconstruct the Dierks reference in order to form a combination with Oka. Even so, as already explained, Oka does not provide what Dierks is missing, i.e., a

teaching or suggestion that “only those signatures generated at a time prior to the certification of the public validation key are recognized as valid.”

Thus even if it were permissible to reconstruct the Dierks reference the rejection must fail because the Oka reference does not disclose the requisite teachings to create the claimed combinations.

The Examiner was requested to provide any basis for disagreement with the above argument in an advisory action and to so provide a full and complete explanation with citation from the prior art in order that Appellants can fully analyze the Examiner’s position prior to appeal. The Advisory Action merely postures as though the Dierks and Oka reference do disclose what is claimed, but the Examiner again fails to reference anything in the Oka reference that suggests the requirement of claim 6 to never permit a certificate to be treated as valid unless

“the signatures generated at a time prior to the certification of the public validation key are recognized as valid.”

The Advisory Action wrongly suggests that support for this subject matter is presented in the Final Office Action. The Examiner has not and cannot find any support in the prior art for this requirement.

For all of these reasons it is urged that the rejection of claim 6 under Section 103 is not properly based and should be overturned.

7A(1)iii REJECTION OF INDEPENDENT CLAIM 18 UNDER SECTION 103 BASED ON DIERKS IN VIEW OF OKA IS ALSO IN ERROR.

Application of the combination of Dierks in view of Oka under Section 103 to claim 18 also results in deficiencies that render the rejection incorrect. The method of claim 18, like claim 6, requires **a certification of the public validation key wherein**

“only those signatures generated at a time prior to the certification of the public validation key are recognized as valid.”

For this reason, Appellants incorporate herein all of the argument presented above with respect to allowability of claim 6 over the same combination. For example, as already noted, in response to Appellants' earlier argument that distinguishes over Dierks, the Final Office Action presented new grounds of rejection relying upon the Oka reference. At page 3, the Final Office Action incorrectly concluded that the Oka reference provides what is missing from the Dierks reference. The rejection mischaracterizes Par. [0152] of Oka, incorrectly asserting Oka teaches:

“that only the signatures generated prior to the certification of the public key are recognized as valid.”

There is no support for this contention and it is only the Appellants who teach this feature.

The rejection goes on to state (see again page 3 of the Final Office Action) that

“the certificate authority (CA) selects signature modules ... and causes the selected the selected modules to generate signatures based on the respective cryptosystems ... before issuing a public key certificate containing the generated signatures.”

Neither the above statement quoted from the Office Action nor any text in the cited paragraph [0152] disclose the above-recited claimed subject matter (which is absent from the Dierks reference). At best, this passage only discloses that modules generate signatures before issuing a certificate. This is not the same as requiring that *only those signatures generated at a time prior to the certification of the public validation key are recognized as valid*.

The Dierks reference at col. 3, lines 51-56 supports Appellants' interpretation that the disclosure of Dierks is limited to the prior art and is expressly inconsistent with the teachings of the Appellants. The passage states that the validation engine has the ability to allow the completion of a requested private key operation by determining

“whether a certificate is treated as valid at that moment or instant in time ...”

Thus the reference does not suggest obtaining a certificate for each request, but only determines whether the certificate is still considered valid. In contrast to such, the invention as defined in independent claim 18 **never** permits a certificate to be treated as valid **unless**

“the signatures generated at a time prior to the certification of the public validation key are recognized as valid.”

The Dierks reference expressly teaches at col. 3, line 67 – col. 4, line 4, that

“the message may only be encrypted if the certificate is valid at the time of encryption ...”

For this reason it would be necessary to reconstruct the Dierks reference in order to form a combination with Oka. That is, the Dierks reference is inconsistent with Appellants' teachings. And Oka does not provide what Dierks is missing, i.e., a teaching or suggestion that “only those signatures generated at a time prior to the certification of the public validation key are recognized as valid.”

Thus even if it were permissible to reconstruct the Dierks reference the rejection must fail because the Oka reference does not disclose the requisite teachings to create the claimed combinations.

The Examiner has failed to provide any basis for disagreement with the above argument. The Advisory Action merely postures as though the Dierks and Oka reference do disclose what is claimed, but the Examiner again fails to find any disclosure in the Oka reference that suggests the requirement of claim 18 wherein

“only those signatures generated at a time prior to the certification of the public validation key are recognized as valid.”

For all of these reasons it is urged that the rejection of claim 18 under Section 103 is error and must be overturned.

7A(1)iii REJECTION OF DEPENDENT CLAIM 12 UNDER SECTION 103 BASED ON DIERKS IN VIEW OF OKA IS ALSO IN ERROR.

The method according to Claim 12 requires, following calculation of the signature and prior to its transfer to a recipient, that

"a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document."

To reject claim 12 the Examiner cites col. 5, lines 29-35 of Dierks, but the above recited language by itself is not the invention. The invention is a combination which includes features not disclosed by the prior art. The combination of features is not present in the references.

7A(1)iv REJECTION OF DEPENDENT CLAIM 23 UNDER SECTION 103 BASED ON DIERKS IN VIEW OF OKA IS ALSO IN ERROR.

The method according to Claim 23 also requires, following calculation of the signature and prior to its transfer to a recipient, that

"a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document."

To reject claim 23 the Examiner again cites col. 5, lines 29-35 of Dierks, as though the above recited language by itself is not the invention. The invention is a combination which

includes features not disclosed by the prior art. The combination of features is not present in the references.

7B(1) REJECTION OF THE DEPENDENT CLAIMS 8, 10, 14, 16, 20 and 22 OVER DIERKS IN VIEW OF OKA AND IN FURTHER VIEW OF WATANABE UNDER SECTION 103 IS IN ERROR.

7B(1)i REJECTION OF DEPENDENT CLAIM 8 OVER DIERKS IN VIEW OF OKA AND IN FURTHER VIEW OF WATANABE UNDER SECTION 103 IS IN ERROR.

According to Claim 8, when certifying the public validation key, a reference to the electronic document is included in addition to a user identifier and the public validation key. The rejection has searched out the Watanabe reference as though it would be obvious to reconstruct the invention by forming a piecemeal combination of prior art components. Many inventions can be formed in hindsight and mere finding and assembling of components is not what determines patentability. Moreover, the futility of this failed attempt is evidenced by the fact that the Watanabe reference (see par. [0010]) does not even disclose the above-recited feature. Rather, the prior art citation merely describes what is attached to the "information submitted by the user" and does not refer to providing a reference to the document when certifying the validation key. The rejection must be overturned.

7B(1)ii REJECTION OF DEPENDENT CLAIM 10 OVER DIERKS IN VIEW OF OKA AND IN FURTHER VIEW OF WATANABE UNDER SECTION 103 IS IN ERROR.

The method of claim 10, which depends from claim 8, further requires that "an implementation of the reference is performed by a calculation of a hash value for the electronic document." In this regard the rejection refers to Watanabe at page 2, par. [0012], but this citation does not refer to use of a hash value for the document. Further, the invention is not simply use of

Serial No. 10/528,312
Atty. Doc. No. 2002P15289WOUS

a hash value, but is a combination of features including those recited in claims 6 and 8. The combination is not taught or suggested. Removal of the rejection is requested.

7B(1)iii REJECTION OF DEPENDENT CLAIM 14 OVER DIERKS IN VIEW OF OKA AND IN FURTHER VIEW OF WATANABE UNDER SECTION 103 IS IN ERROR.

According to Claim 14, following calculation of the signature and prior to its transfer to a recipient, "a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document." The claimed subject matter is more than performing a validation, but rather, is a combination of features. The rejection refers to Dierks at col. 3, but overlooks that the preceding lines 5-9 of col. 3 in Dierks teaches against the invention, by stating that the validity of a certificate is determined by the relying party at the time of reliance "subject to any error windows resulting from a delay in updating validity information." **To the contrary, Appellants require that**

"only those signatures generated at a time prior to the certification of the public validation key are recognized as valid."

That is, provision of validity information "post certification" is precluded by this claim.

7B(1)iv REJECTION OF DEPENDENT CLAIM 16 OVER DIERKS IN VIEW OF OKA AND IN FURTHER VIEW OF WATANABE UNDER SECTION 103 IS IN ERROR.

According to Claim 16, following calculation of the signature and prior to its transfer to a recipient, "a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document." The claimed subject matter is more than performing a validation. It is a combination of features. The rejection refers to Dierks at col. 3, but overlooks that lines 5-9 of col. 3 in Dierks teaches against the invention, by stating that the validity of a certificate is determined by the relying party at the time of reliance

"subject to any error windows resulting from a delay in updating validity information." To the contrary, Appellants require that

"only those signatures generated at a time prior to the certification of the public validation key are recognized as valid."

That is, provision of validity information "post certification" is precluded by claim 16.

7B(1)v REJECTION OF DEPENDENT CLAIM 20 OVER DIERKS IN VIEW OF OKA AND IN FURTHER VIEW OF WATANABE UNDER SECTION 103 IS IN ERROR.

According to Claim 20, "when certifying the public validation key, at least one reference to the electronic document, of which there is at least one, is included in addition to a user identifier and the public validation key." As done for claim 6, the rejection has searched out the Watanabe reference as though it would be obvious to reconstruct the invention by piecemeal recombination. But the Watanabe reference (see par. [0010]) does not disclose the above-recited feature. Rather, the prior art citation merely describes what is attached to the "information submitted by the user" and does not refer to providing a reference to the document when certifying the validation key. Reversal of the rejection of claim 8 is requested.

7B(1)vi REJECTION OF DEPENDENT CLAIM 22 OVER DIERKS IN VIEW OF OKA AND IN FURTHER VIEW OF WATANABE UNDER SECTION 103 IS IN ERROR.

The method of claim 22, which depends from claim 20, further requires that "an implementation of the reference, of which there is at least one, takes place by means of a calculation of a hash value for the electronic document, of which there is at least one." The rejection relies upon Watanabe at page 2, par. [0012], but this citation does not refer to use of a hash value for the document. Further, the invention is not simply use of a hash value, but is a combination of features including those recited in claims 18 and 20. The combination is not taught or suggested. Removal of the rejection is requested.

7C. CONCLUSIONS

Argument has been presented to demonstrate that all of the rejections under Section 103 are deficient and that the dependent claims further distinguish over the prior art. The Examiner has argued rejections when claimed features are absent from the references and not suggested by the prior art. The Examiner has written argument "as though" cited text contains the claimed subject matter, but a plain reading of the cited prior art text clearly shows that the rejections are without basis. Accordingly, none of the rejections can be sustained. For all of the above-argued reasons, all of the rejections should be overturned and the claims should be allowed.

8. APPENDICES

An appendix containing a copy of the claims involved in this appeal is provided herewith. No evidence appendix or related proceedings appendix is provided because no such evidence or related proceeding is applicable to this appeal.

Respectfully submitted,

Dated: 7/23/08

By: 

John P. Musone
Registration No. 44,961
(407) 736-6449

Siemens Corporation
Intellectual Property Department
170 Wood Avenue South
Iselin, New Jersey 08830

9. APPENDIX OF CLAIMS ON APPEAL

6. A method for generating and/or validating electronic signatures, the method comprising:
- generating an asymmetrical key pair which includes a private signature key and a public validation key;
 - calculating an electronic signature for an electronic document by means of the private signature key and by applying a predeterminable signature function; and
 - performing a certification of the public validation key wherein, when validating, only those signatures generated at a time prior to the certification of the public validation key are recognized as valid.
8. The method according to Claim 6, wherein, when certifying the public validation key, a reference to the electronic document is included in addition to a user identifier and the public validation key.
10. The method according to Claim 8, wherein an implementation of the reference is performed by a calculation of a hash value for the electronic document.
12. The method according to Claim 6, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document.
14. The method according to Claim 8, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document.
16. The method according to Claim 10, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document.

18. A method for generating and/or validating electronic signatures, the method comprising:
- generating an asymmetrical key pair which includes a private signature key and a public validation key;
 - calculating at least one electronic signature for at least one electronic document by means of the private signature key and by applying a predeterminable signature function; and
 - following calculation of the electronic signature, of which there is at least one, carrying out a certification of the public validation key wherein only those signatures generated at a time prior to the certification of the public validation key are recognized as valid.
20. The method according to Claim 18, wherein, when certifying the public validation key, at least one reference to the electronic document, of which there is at least one, is included in addition to a user identifier and the public validation key.
22. The method according to Claim 20, wherein an implementation of the reference, of which there is at least one, takes place by means of a calculation of a hash value for the electronic document, of which there is at least one.
23. The method according to Claim 18, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, of which there is at least one, in order to verify an action of intent which is expressed by the electronic document, of which there is at least one.

Serial No. 10/528,312
Atty. Doc. No. 2002P15289WOUS

10. EVIDENCE APPENDIX - 37 CFR 41.37(c) (1) (ix)

None

Serial No. 10/528,312
Atty. Doc. No. 2002P15289WOUS

11. RELATED PROCEEDINGS APPENDIX - 37 CFR 41.37(c) (1) (x)

None